UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,918	12/12/2001	Louis Guillou	9320.134USWO	3008

23552 7590 05/03/2005

MERCHANT & GOULD PC
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/889,918	GUILLOU ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/25/03, 12/12/01*.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *3/28/05, 4/4/05*.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 10/19/2004.

DETAILED ACTION

1. Claims 1-18 have been examined.

Title

2. The title of the invention is acceptable.

Priority

3. This application is a 371 of PCT/FR00/00190 filed 01/27/2000 claiming priority to France applications 99/12465, 99/12467, and 99/12468 filed 10/01/1999 and France application 99/03770 filed 03/23/1999 and France application 99/01065 filed 01/27/1999.

4. The effective filing date for the subject matter defined in the pending claims in this application is 01/27/1999.

Information Disclosure Statement

5. The information disclosure statements (IDS) submitted on 02/25/2003 and 12/12/2001 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

6. The subject matter of this application admits of illustration by a drawing to facilitate understanding of the invention. Applicant is required to furnish a drawing under 37 CFR 1.81(c). No new matter may be introduced in the required drawing. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d).

Specification

7. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.

(b) CROSS-REFERENCE TO RELATED APPLICATIONS.

(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.

(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT

(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or

REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)

(f) BACKGROUND OF THE INVENTION.

(1) Field of the Invention.

(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.

(g) BRIEF SUMMARY OF THE INVENTION.

(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).

(i) DETAILED DESCRIPTION OF THE INVENTION.

(j) CLAIM OR CLAIMS (commencing on a separate sheet).

(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).

(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

8. These section headings must be added to the specification as well as a brief description of the drawings which also need to be added. Also, a detailed description of the newly added drawings must be added to the specification.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Due to the numerous 112 issues and the fact that they were all discussed with the applicant in the interview on 3/28/2005, each individual rejection will not be discussed below. However, this does not relieve the applicant from fixing these errors in accordance with the discussion held on 3/28/2005. These errors include antecedent basis issues, preamble issues, gerund issues in method step claims, the "and/or" issues, duplicate heading statement issues, and any other issues discussed during the interview on 3/28/2005. Correction is required.

Claim Rejections - 35 USC § 101

12. Claims 1-3 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-3 recite a method of authentication involving a good number of steps. However, there are no statutory limitations presented in any of these claims. The claim steps deal with mathematics and manipulation of numbers and as such could be accomplished between two people talking directly to each other. All of the calculations could potentially be done in the participants' heads without the aide of any statutory object and the communications can be accomplished through speech. Furthermore, the message does not make the claims statutory because the message could be as simple as a spoken word. As such, these claims fail to meet the statutory requirement of 35 USC 101 and are therefore rejected.

Allowable Subject Matter

13. Claims 1-18 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, and the rejection(s) under 35 U.S.C. 101, set forth in this Office action.

14. The following is a statement of reasons for the indication of potentially allowable subject matter:

15. The invention relates to a method (Claim 1) and a system (Claims 6 and 11) for proving, to a verification entity, the authenticity of an entity and/or the integrity of a message associated with said entity, comprising the following sequential steps: the entity carries out a commitment process; the verification entity issues a challenge; the control entity issues a response and the verification entity verifies said response. The invention also relates to a verification device (Claim 15) using said method.

16. Prior art: Document EP-A-O 311 470, cited in the application, describes a similar method wherein an entity designated as a "trusted authority" assigns an identity to each entity designated as "control" and calculates the RSA signature thereof; in the course of the personalization procedure, the trusted authority provides the identity and signature to the control, where after the control entity declares: "Here is my identity; I know the RSA signature thereof". The control thus providing proof of knowledge of the RSA signature of the stated identity without disclosing said signature. Using the RSA verification public key distributed by the trusted authority, an entity designated as "verification entity" verifies that the RSA signature corresponds to the stated identity without seeing said signature. The mechanisms using this protocol take place without any "transfer of knowledge": the control entity does not know the RSA private key used by the trusted authority to sign a large number of identities.

17. The problem: The use of RSA technology opens up the authentication method to so-called "multiplicative" attacks. Moreover, the workload involved in the arithmetic

operations requires computation times that are far too high for smart card-type applications.

18. The invention: The method does not use the RSA signature, and computes commitments R, challenges d and responses R on the basis of public/private keys and Qs, as defined by the features of Claim 1.

19. None of the documents cited in the international search report or in the attached 892 discloses or suggests the computation steps as defined in Claim 1. In particular, document EP-A-O 792 044, although it relates to a challenge/response type authentication method, uses the RSA technology, and therefore fails to disclose the combination of limitations as claimed in Claim 1. Therefore, the subject matter as claimed in claim 1 distinguishes over the prior art.

20. Independent Claims 6 and 11 are equivalent to Claim 1, and relate to systems comprising the control device computing the commitments, receiving the challenges and computing the responses. They therefore also distinguish over the prior art.

21. Independent Claim 15 relates to a control device which computes Gi and Qs values as per the method of the invention. Since said computations in the combination as claimed are neither disclosed nor suggested by the cited documents, said claim also distinguishes over the prior art.

22. Because claims 2-5, 7-10, 12-14, and 16-18 further limit the independent claims, they too distinguish over the prior art.

Conclusion

23. Claims 1-18 have been rejected.

24. The applicant is reminded that a larger font size as well as a mono-spaced font would be helpful to in the publishing of this application upon allowance due to the sub/super-scripting throughout the specification and the claims.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Matthew Henning
Assistant Examiner
Art Unit 2131
4/12/2005